
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION

In the Matter of the Search of a Cellular
Telephone _____, Cellular
Number _____

**MEMORANDUM DECISION
REGARDING ISSUANCE OF AN 18
U.S.C. § 2703 WARRANT AND A
PING WARRANT**

Case No. 2:19-mj-00759

Magistrate Judge Evelyn J. Furse

The Government requested a search and seizure warrant for cellular telephone subscriber information, historical and prospective location information for the cellular telephone, a pen register and trap and trace device, and the ability to demand the cellular telephone company affirmatively “ping” the particular cellular telephone to obtain its location at the will of the agents in an ongoing criminal investigation. The Assistant United States Attorney presented the application for a search and seizure warrant seeking all of these tools pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A), 3121-3127. A Special Agent for the Federal Bureau of Investigation signed the search and seizure warrant application and the accompanying affidavit.

The Court found probable cause to believe the cellular telephone subscriber committed a federal crime and probable cause to believe that the requested warrant would reveal his/her location. The Court signed a search and seizure warrant authorizing subscriber information and seven days of historical location information.

The Court provided a tracking warrant and All Writs Act authorization for the thirty days of prospective location information and the ability to “ping” the cellular telephone.

Following the issuance of these warrants, the Court has taken the opportunity to consider further the request and the appropriate vehicles for such authorizations. In doing so the Court concludes as follows. A warrant ordering an electronic communications service or a remote computing service to provide any kind of information is an 18 U.S.C. § 2703 warrant. A 2703 warrant for prospective location information should employ the procedures associated with a tracking warrant. A 2703 warrant for historical location information and subscriber information should employ the procedures associated with a search and seizure warrant. The All Writs Act, not 18 U.S.C. § 2703, provides the authority for the Court to issue a ping warrant, and it should employ the procedures associated with a tracking warrant.

I. BACKGROUND

The investigation began in May 2019 with a traffic stop. One of the people in the vehicle had a cellular telephone that police seized and obtained a search and seizure warrant to search. The search of the phone produced evidence of federal crimes. The Special Agent sought subscriber information, seven days of historical location information, thirty days of prospective location information, a pen register and trap and trace device, and the ability to “ping” the cellular telephone. The affidavit further requests authorization of execution of the warrant at any time of the day or night because of “the potential need to locate the Target Cell Phone outside of daytime hours.”

In requesting location information, the warrant application requested cell-site information, E-911 Phase II data, Timing Advance information, and True Call data. The affidavit in support of the application, indicates that the cell-site information provides the general location of the cellular telephone based on the tower(s) that communicated with the phone at a given time. The E-911 Phase II data provides Global Position Service (GPS) data or latitude-longitude data, which provides greater precision than the cell-site information. According to Wikipedia, the Timing Advance information includes the length of time a cell signal takes to travel from the base station to the mobile device and can allow localization and tracking of the device. Timing advance, Wikipedia, https://en.wikipedia.org/wiki/Timing_advance (last visited Dec. 23, 2019). TrueCall is a geoanalytic platform used by service providers for a variety of reasons including to provide precise location information. TrueCall, Netscout, <https://www.netscout.com/product/truecall> (last visited Dec. 23, 2019).

According to the affidavit a “ping” occurs when the cellular telephone company initiates a signal to determine the location of the target cellular telephone on the company’s network or other reference points, including E-911 Phase II data, as available.

The Court refrains from providing further detail about the investigation because it does not know the status of the investigation at this time.

II. ANALYSIS

In Carpenter v. United States, 585 U.S. ___, 138 S. Ct. 2206, 2221 (2018), the Supreme Court ruled that law enforcement had to obtain a warrant supported by probable cause to acquire historical cell site location information. The majority

specifically withheld judgment on real-time cell site location information. Id. at 2220. Our existing forms for search and seizure warrants and tracking warrants do not contemplate the state of the law post-Carpenter. This decision concerns the warrants issued as they differ from that requested by the Special Agent. This Court has spent significant time since Carpenter trying to determine the appropriate avenue to authorize seizure of prospective location information and has repeatedly asked the Assistant United States Attorneys appearing in front of it for support for their requests for such information through standard search and seizure warrants and has reached the following conclusions.

A. A Warrant Ordering an Electronic Communications Service or a Remote Computing Service to Provide Any Kind of Information is an 18 U.S.C. § 2703 Warrant

The Stored Communication Act authorizes warrants seeking information from an electronic communications service or a remote computing service and differ from those provided for by 18 U.S.C. §§ 3102, 3117 and Federal Rule of Criminal Procedure 41. The Stored Communication Act authorizes law enforcement to, among other things, obtain a warrant from a federal court for information collected by an electronic communications service or a remote computing service. 18 U.S.C. § 2703(c)(1)(A). The warrant “issue[s] using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction.” Id. Companies providing cellular telephone services, including the one as alleged in this matter, constitute electronic communications services and/or remote computing services. 18 U.S.C. §§ 2510(15), 2711(2).

Under Federal Rule of Criminal Procedure 41, to issue either a search or tracking warrant, a magistrate judge must have probable cause to believe a specific crime has been committed and that law enforcement will find evidence of that crime, contraband, property designed for the crime, or the person to be arrested in the place they intend to search or by tracking the location of something. Fed. R. Crim. P. 41(c) & (d)(1). Rule 41 explicitly acknowledges it does not modify any statute. Fed. R. Crim. P. 41(a)(1).

18 U.S.C. § 2703 specifically creates a warrant separate and distinct from the search and seizure warrants created by 18 U.S.C. § 3102 and tracking warrants created by 18 U.S.C. § 3117. Prior to Carpenter, a number of opinions struggled with whether requests for location information under 18 U.S.C. § 2703 required issuance of warrant or simply an order, and if these requests required warrants, whether they required search and seizure warrants or tracking warrants. See In re Order Authorizing Prospective & Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889 (S.D. Tex. 2014) (finding requests for prospective, continuous, and contemporaneous cellular telephone location information constitute a request for a tracking warrant); In re Smartphone Geolocation Data Appl., 977 F. Supp. 2d 129, 150 (E.D.N.Y. 2013) (finding requests for prospective, continuous, and contemporaneous cellular telephone location information constitute a request for a search and seizure warrant); In re Appl. of United States for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 448-49 (S.D.N.Y. 2005) (finding requests for prospective, continuous, and contemporaneous cellular telephone location information constitute requests for an order under 18 U.S.C. § 2703 and the pen register statute and thus do not require a warrant).

In light of Carpenter, 138 S. Ct. at 2221, we now know law enforcement must obtain a warrant to receive historical location information from cellular telephone companies. Most Assistant United States Attorneys now seek warrants supported by probable cause to obtain prospective location information from cellular telephone companies citing both 18 U.S.C. § 2703 and Federal Rule of Criminal Procedure 41. No form from the Administrative Office of the Courts exists for this type of warrant, and so courts generally issue either search and seizure warrants or tracking warrants under Federal Rule of Criminal Procedure 41 with citations to relevant statutes in the application and sometimes in the attachments to the warrant itself. These forms are a poor fit because the warrants authorized by 18 U.S.C. § 2703 do not fall neatly under Rule 41, and indeed, the statute supersedes the Rule.

First, Federal Rule of Criminal Procedure 41 does not contain the authority necessary to order an out of district electronic communications service and/or remote computing service to comply with the warrant, thus the forms fail to identify the basis for extra-district authority. 18 U.S.C. § 3102 and Federal Rule of Criminal Procedure 41 only authorize a magistrate judge to issue a search and seizure warrant for a person or property within her district, or at least within her district at the time of issuance, except in a terrorism investigation or investigation related to United States' properties outside of any federal district or where a person concealed the location of electronically stored information or in a computer fraud investigation with damaged computers in at least five districts. Fed. R. Crim. P. 41(b). A tracking warrant offers a slightly larger geographic scope. A magistrate judge can only order installation of a tracking device within the district in which she sits. 18 U.S.C. § 3117(a); Fed. R. Crim. P. 41(b)(4). However,

once installed, the agents may track the device inside or outside the district. Id. By contrast to both of these warrants, a warrant issued under 18 U.S.C. § 2703 to an electronic communications service and/or remote computing service (i.e., a cellular telephone provider) may issue from any district with jurisdiction over the offense or the provider. 18 U.S.C. § 2711(3)(A). The location of the cellular phone or the cellular telephone company remains irrelevant. The standard forms for search and seizure warrants and tracking warrants lack any indication of their extra-district application of the legal basis for their geographic reach.

Second, Rule 41 requires execution of a search and seizure warrant within fourteen days, and the agent must provide the return promptly after execution. Fed. R. Crim. P. 41(e)(2)(A) & (f)(1)(D). If the warrant calls for electronically stored information, “[t]he time for executing the warrant . . . refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.” Fed. R. Crim. P. 41(e)(2)(B). Thus when an application uses a search and seizure warrant form pursuant to Rule 41, the Court can only authorize a maximum of fourteen days of prospective location data, absent modification of the form. Requests for prospective location information to electronic communications services and remote computing services regularly exceed the fourteen-day limit. Rule 41 does not contain any provision to extend the time for execution of a search and seizure warrant.

Third, while a tracking warrant allows a longer period of data collection, it by definition cannot apply to information collected by cellular telephone companies. A number of courts have identified problems with considering a cellular telephone a tracking device. See United States v. Ackies, 918 F.3d 190, 199 (1st Cir. 2019) (holding

a cell phone not a tracking device under 18 U.S.C. § 3117 because the statute refers to “installation”, and tracking of a cell phone requires no installation as location information is readily available to the cellular telephone company, the Advisory Committee Notes accompanying the statute differentiates it from monitoring governed by the Stored Communications Act, determining current location of the cell phone may prove impossible, and Fed. R. Crim. P. 41 calls for “maintenance” and “removal” of a tracking device, which also does not apply to a cellular telephone); In re Appl. of the United States for an Order for Authorization to Obtain Location Data Concerning an AT & T Cellular Tel., 102 F. Supp. 3d 884, 892 (N.D. Miss. 2015) (finding “the ‘installation’ language in the Tracking Device Statute constitutes a real reason for not utilizing that statute for requests for prospective cell phone location data”); In re Smartphone Geolocation Data Appl., 977 F. Supp. 2d 129, 150 (E.D.N.Y. 2013) (finding reading a tracking device to include cellular telephones in conflict with legislative history regarding the meaning of tracking device, inconsistent with the plain language of the statute requiring “installation” of a “device”, and illogically and unworkably broad). To the extent a tracking warrant seems more appropriate despite the in-district installation requirement noted above, an electronic communication, by statutory definition, excludes “any communication from a tracking device (as defined in section 3117 of this title).” 18 U.S.C. § 2510(12)(C). And an electronic communication service, covered by 18 U.S.C. § 2703, is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). Thus, if a cellular telephone qualifies as a tracking device under 18 U.S.C. § 3117, then the Stored Communications Act excludes cellular telephone communications and companies from coverage.

However, Congress definitely wrote the Stored Communications Act to apply to cellular telephone companies. S. Rep. No. 541, S. REP. 99-541, 16, 1986 U.S.C.C.A.N. 3555, 3568 & 3570. Thus, courts cannot consider warrants to electronic communications services and/or remote computing services for prospective location data tracking warrants without causing the Stored Communications Act to no longer apply to those entities, thus depriving the courts of extra-district authority.

All of these concerns dissipate when one reads 18 U.S.C. § 2703 as authorizing a distinct type of warrant issuable to electronic communication services and/or remote computing services that it may use the procedures of Rule 41 to issue, hereinafter a 2703 warrant. 18 U.S.C. § 2703(c)(1)(A).

B. A 2703 Warrant for Prospective Location Information Should Employ the Procedures Associated with a Tracking Warrant

Because 18 U.S.C. § 2703(c)(1)(A) directs courts to employ the procedures in the Federal Rules of Criminal Procedure and prospective location information most closely resembles information typically sought by a tracking warrant, this courts will employ the relevant portions of Rule 41 regarding tracking warrants. In discussing historical cell site location information, the Carpenter court acknowledged the similarity between historical location information and GPS trackers: “Such tracking partakes of many of the qualities of the GPS monitoring we considered in [United States v. Jones, 565 U.S. 400 (2012)]. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.” Carpenter, 138 S. Ct. at 2216. The tracking discussed in Jones requires the issuance of a tracking warrant. See Jones, 565 U.S. at 402-03, 404 (noting government initially obtained a tracking

warrant but failed to comply with the conditions of the warrant and finding installation of a tracking device on a private vehicle constituted a search).

The location information sought in this warrant includes GPS tracking of the phone, which by nature of coming through a cellular telephone “achieves near perfect surveillance, as if [the recipient] had attached an ankle monitor to the phone’s user.” Carpenter, 138 S. Ct. at 2218. Indeed, the affidavit makes clear that the Special Agent seeks the warrant to determine the location of the phone and thus the person carrying the phone. C.f. United States v. Werdene, 883 F.3d 204, 211 (3d Cir. 2018) (finding a Network Investigative Technique (NIT) not a tracking warrant where “[t]he explicit purpose of the warrant was not to track movement—as would be required under Rule 41(b)(4)” (emphasis in original)). In general, a tracking warrant issues where law enforcement seeks evidence of a crime, contraband, property designed for the crime, or a person to be arrested by use of the tracking warrant. 18 U.S.C § 3117; Fed. R. Crim. P. 41(d) & (e)(2)(C). Law enforcement clearly seeks prospective location information from the cellular telephone company for this same purpose.

Furthermore, a tracking warrant requires agents to install a tracking device within ten days of the magistrate judge signing the warrant, may track the device for forty-five days, and the agent must provide the return within ten days after use of the tracking device ends. Fed. R. Crim. P. 41(e)(2)(C) & (f)(2)(B). Additionally, the court may extend the use of a tracking device for good cause. Fed. R. Crim. P. 41(e)(2)(C). By contrast, a search and seizure warrant can authorize a search for no longer than fourteen days from the date of signature. Fed. R. Crim. P. 41(e)(2)(A) & (B). Any extension of that time period would require a new warrant. The tracking warrant

procedures transfer well to authorization for prospective location information from a cellular telephone company. The Agents should serve the 2703 warrant for prospective location information within ten days of signature; the 2703 warrant can allow up to forty-five days of tracking, subject to extension for good cause; and the agents must file the return within ten days of ceasing tracking.

This warrant also incorporated a request for prospective pen register and trap and trace information. To the extent agents choose to use a warrant to request such information, they should likewise follow the procedure outlined above for such prospective information.

C. A 2703 Warrant for Historical Location Information and Subscriber Information Should Employ the Procedures Associated with a Search and Seizure Warrant

Because 18 U.S.C. § 2703(c)(1)(A) directs courts to employ the procedures in the Federal Rules of Criminal Procedure and historical location information most closely resembles information typically sought by a search and seizure warrant, this court employs the relevant portions of Rule 41 regarding search and seizure warrants. When agents seek historical location information from electronic communications services or remote computing services that already exists at the time the magistrate judge signs the warrant, Rule 41 search and seizure warrant procedures meet their needs. The Rule requires execution of the warrant within fourteen days of signature, and agents must complete execution by collecting all relevant material from the warrant recipient and may view it offsite at a later date. Fed. R. Crim. P. 41(e)(2)(A) & (B). Section 2703 makes clear that the executing agent need not appear in person at the electronic communications service or stored computer service to execute the warrant. 18 U.S.C. §

2703(g). Under Rule 41, the agent must “promptly” provide the return to the magistrate judge. Fed. R. Crim. P. 41(f)(1)(D). Agents can easily follow these procedures with respect to historical location information.

This warrant also incorporated a request for subscriber information. To the extent agents choose to use a warrant to request such information, they should likewise follow the procedure outlined above for such historical information.

D. A Ping Warrant Requires All Writs Act Order

None of the statutes discussed so far provides the Court with authority to require a cellular telephone company to ping a phone, and the Court can only order such under the All Writs Act. The warrant at issue in this case also seeks the ability for the Special Agent to order the cellular telephone company to ping the cellular telephone at will to assist in determining its location. Search and seizure warrants generally allow law enforcement to collect evidence already in existence, where an anticipatory warrant or a tracking warrant authorize the collection of evidence to be created by the defendant’s actions in the near future. A ping warrant does something distinctly different. A ping warrant orders a cellular telephone company to affirmatively create evidence about the whereabouts of a particular cellular telephone at the direction of law enforcement.

The Pen Register and Trap and Trace Statute contains provisions that require the recipient of a pen register order to “furnish . . . all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services.” 18 U.S.C. § 3124(a). The statute also requires the recipient of a trap and trace order to “furnish . . . all additional information, facilities, and technical assistance including installation and

operation of the device unobtrusively and with a minimum of interference with the services.” 18 U.S.C. § 3124(b). The Stored Communications Act requires a recipient “to disclose a record or other information pertaining to a subscriber to or customer of such service.” 18 U.S.C. § 2703(c). None of these authorizations involves this type of affirmative participation in an investigation. To obtain that authority, one must turn to the All Writs Act.

Indeed, prior to enactment of the Pen Register and Trap and Trace Statute, the Supreme Court found courts had to draw authority to order a telephone company to assist in installing a pen register from the All Writs Act because neither the statutes at the time nor Federal Rule of Criminal Procedure 41 gave authority to order third-party assistance. United States v. New York Tel. Co., 434 U.S. 159, 172-77 (1977). The All Writs Act enables federal courts to “issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U.S.C. § 1651. “The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, ..., and encompasses even those who have not taken any affirmative action to hinder justice.” New York Tel. Co., 434 U.S. at 174 (internal citations omitted); see accord United States v. Velarde, 485 F.3d 553, 560 (10th Cir. 2007) (finding All Writs Act affords “a district court . . . broad discretion to fashion discovery mechanisms suitable to the case before it.”). While the All Writs Act provides broad authority to federal courts, “the power of federal courts to impose duties upon

third parties is not without limits; unreasonable burdens may not be imposed.” New York Tel. Co., 434 U.S. at 172.

In this instance, 18 U.S.C. § 2703 read in conjunction with Carpenter and Jones allows for law enforcement to use cellular telephones to track evidence of crimes, including the location of those suspected of committing them. See Carpenter, 138 S. Ct. at 2221 (requiring law enforcement to obtain a warrant to acquire historical cell site location information); Jones, 565 U.S. at 404 (requiring law enforcement to obtain a warrant before attaching a tracking device to a vehicle to acquire GPS data). Probable cause exists to believe that pinging this phone will reveal the location of the suspect for whom probable cause exists to believe s/he committed a feral offense. According to the Affidavit accompanying the warrant, the cellular telephone company has the ability to ping telephones in its network and can do so without an unreasonable burden. If the cellular telephone company disagrees, it can always move to quash the warrant. Furthermore, a ping is less intrusive than a search of a home or business, which the court could authorize to find a suspect. Where a court could order the search of a home or a business for a suspect on a showing of probable cause, authorization of the lesser intrusion of a ping based on probable cause would be “agreeable to the usages and principles of law.” 28 U.S.C. § 1651; see New York Tel. Co., 434 U.S. at 176-77. A failure to authorize the ping would frustrate the proper administration of justice.

Therefore the Court finds the All Writs Act provides the authority necessary for the Court to issue a ping warrant in connection with a 2703 warrant for prospective location information. The Court imposes similar Rule 41 limitations on ping warrants to keep application consistent with “the usages and principles of law”. 28 U.S.C. § 1651.

Agents should serve the ping warrant within ten days of signature; the warrant will allow forty-five days of tracking, subject to extension for good cause; and the agents must file the return within ten days of ceasing tracking.

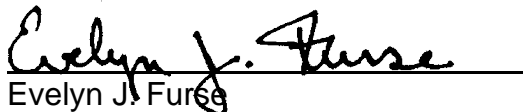
III. Conclusion

Given the recent legal developments with respect the legal process required to obtain historical cell site information, the existing processes and forms for search and seizure warrants and tracking warrants fail to cover the ground necessary to authorize warrants under 18 U.S.C. § 2703 and ping warrants. This opinion aims to clarify the basis for the warrants authorized and the process it intends to follow for such requests.

In short, a warrant ordering an electronic communications service or a remote computing service to provide any kind of information is a 2703 warrant. A 2703 warrant for prospective location information should employ the procedures associated with a tracking warrant. A 2703 warrant for historical location information and subscriber information should employ the procedures associated with a search and seizure warrant. The All Writs Act, not 18 U.S.C. § 2703, provides the authority for the Court to issue a ping warrant, and it should employ the procedures associated with a tracking warrant.

DATED this 26th day of December, 2019.

BY THE COURT:


Evelyn J. Furse
United States Magistrate Judge